IN THE UNITED STATES DISTRICT COURT
FOR DISTRICT OF MONTANA

| | |
|---|---|
| IN THE MATTER OF THE SEARCH OF:<br><br>Black Samsung phone in clear case, IMEI: 358284143661740 (Device 1); Black Samsung phone, IMEI: 353021070606008 (Device 2); Silver HP computer, model Elite X2, Serial number: CND122ONHS (Device 3), that are currently in the Yellowstone County Sheriff's Office evidence vault. | Case No. MJ-24-68-BIG-TJC |

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE**

I, Bethany A. Richter, being first duly sworn, hereby depose and state as follows:

## INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of the following three devices: Black Samsung phone in clear case, IMEI: 358284143661740 (Device 1); Black Samsung phone, IMEI: 353021070606008 (Device 2); Silver HP computer, model Elite X2, Serial number: CND122ONHS (Device 3), that are currently in the Yellowstone County Sheriff's Office evidence vault, hereafter referred to as "Device 1", "Device 2", "Device 3", and supported with photographs which are currently in law enforcement possession for the seizure and search of the items described in Attachment A and the subsequent seizure of items described in Attachment B, including electronically stored evidence.

2. I, Detective/TFO Bethany Richter, have been employed full time with the Yellowstone County Sheriff's Office since 2013 and am currently assigned to the Detective Division. I attended the MT Law Enforcement Academy and through continuing education and training have obtained my Basic, Intermediate, Advanced, and Supervisory Certifications from the Montana Peace Officer's Standards and Training Council (POST). I earned a bachelor's degree in psychology from the University of Great Falls. I have worked as a Federal Task Force Officer for the FBI's Montana Child Exploitation and Human Trafficking Task Force (MTCEHTTF) since July 2022.

I have specialized training in Interview and Interrogation, Body Language, Drug Interdiction Training, Hostage Negotiation, Homicide Investigation, Shooting Reconstruction, Bloodstain Pattern Analysis and Crisis Intervention. I am a certified Drug Recognition Expert. I have conducted hundreds of investigations throughout my career including assault, drug possession, homicide, crimes against children, sex offenses, and such. I have also pursued criminal violations in the Montana District Court and United States Federal Court. I am assigned the investigation described in the following paragraphs and the information contained in this affidavit is based on my own observations, interviews with witnesses, my training and experience, and information provided to me by other task force members or other law enforcement officers.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

## RELEVANT STATUTES

4. This investigation concerns alleged violations of the following criminal statutes (summarized):

- 18 U.S. Code § 2423(b) A person who travels in interstate commerce or travels into the United States, or a United States citizen or an alien admitted for permanent residence in the United States who travels in foreign commerce, with a motivating purpose of engaging in any illicit sexual conduct with another person shall be fined under this title or imprisoned not more than 30 years, or both.

- 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer.

- 18 U.S.C. § 2252A(a)(2) prohibits a person from knowingly receiving or distributing any child pornography using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer or any material that contains child pornography using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

## TECHNICAL TERMS

5. Based on my training and experience, the affiant uses the following technical terms to convey the following meanings:

a. **Computer:** includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, smartphones, mobile phones, tablets, server computers, and network hardware.

b. **Wireless telephone:** A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice

communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

c. **Data:** means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device.

d. **Digital camera:** is a device that records and stores photographic images in digital form that can be transferred to a computer as the impressions are recorded or stored in the camera for later loading into a computer or printer. Wireless telephones more often than not possess an integrated digital camera.

e. **Email** or **electronic mail:** means messages transmitted over communications networks. The messages can be notes entered from the keyboard or electronic files stored on disk. Most mainframes, computer networks, and minicomputers have an email system. Sent messages are stored in electronic mailboxes at least until the recipient retrieves them. After reading electronic mail, recipients can store it on their computer as a file, forward it to other users, or delete it, or they may store the message on a remote server, such as the one from which they may have retrieved the email.

f. **Flash medium:** is any data repository that uses flash memory cells, which can be electronically erased and reprogrammed and does not need power to retain data.

g. **Image** or **copy:** refers to an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. "Imaging" or "copying" maintains contents, but attributes may change during the reproduction.

h. **Internet:** is a global network of computers and other electronic devices that communicate with each other via standard telephone lines, high-speed telecommunications links (e.g., fiber optic cable), and wireless transmissions. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. **Text Messages:** are a form of communication through the use of cellular telephones or handheld electronic devices upon an electronic service provider's network or system. A message normally contains text composed by

the sender, usually input via a lettering system on the device or computer's keypad. The message can also be an image or short video sent or received.

j. **Uniform Resource Locator:** (URL) are typically used to access web sites or other services on remote devices such as http://www.usdoj.gov, for example.

k. **Voice Mail:** means a computerized system for answering incoming phone calls and allowing the caller to leave a message, which may be later retrieved.

l. **World Wide Web:** can be considered a massive database of information that is stored on linked computers that make up the Internet. This information can be displayed on a computer in the form of a web page, which is a document on the World Wide Web. A web site is a related collection of files and can consist of any number of web pages.

6. Based on my training, experience, and research, the affiant knows that smartphone devices have capabilities that allow them to serve as a wireless telephone and digital camera that connects to the Internet. In the affiant's training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, who the user was communicating with, and content of those communications.

7. Based upon my knowledge, training, and experience in child exploitation and human trafficking investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I am aware of the following:

## PROCEDURES FOR ELECTRONICALLY STORED INFORMATION AS TO ANY CELLULAR TELEPHONE

a. It is not possible to determine, merely by knowing the cellular telephone's make, model and serial number, the nature and types of services to which the device is subscribed and the nature of the data stored on the device. Cellular devices today can be simple cellular telephones and text message devices, can include cameras, can serve as personal digital assistants and have functions such as calendars and full address books and can be mini-computers allowing for electronic mail services, web services and rudimentary word processing. An increasing number of cellular service providers

now allow for their subscribers to access their device over the internet and remotely destroy all of the data contained on the device. For that reason, the device may only be powered in a secure environment or, if possible, started in "airplane mode" which disables access to the network. Unlike typical computers, many cellular telephones do not have hard drives or hard drive equivalents and store information in volatile memory within the device or in memory cards inserted into the device. Current technology provides some solutions for acquiring some of the data stored in some cellular telephone models using forensic hardware and software. Even if some of the stored information on the device may be acquired forensically, not all of the data subject to seizure may be so acquired. For devices that are not subject to forensic data acquisition or that have potentially relevant data stored that is not subject to such acquisition, the examiner must inspect the device manually and record the process and the results using digital photography. This process is time and labor intensive and may take weeks or longer.

b. Following the issuance of this warrant, the Devices will be sent to another location, most likely out of the State of Montana, to be subjected to a forensic analysis. All forensic analyses of the data contained within the telephone and its memory cards will employ search protocols directed exclusively to the identification and extraction of data within the scope of this warrant and will follow the procedures below.

c. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

d. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

8. Based on her knowledge, training, and experience, the affiant knows that electronic devices can store information for long periods of time. Similarly, items that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

9. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on these Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. The affiant knows that when an individual uses an electronic device to facilitate human trafficking, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of facilitating the criminal offense, for example, communicating with victims or customers in a commercial sex scheme. The electronic device is also likely to be a storage medium for evidence of crime. From his training and experience, the affiant believes that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

10. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant the affiant is applying for would permit an agent's seizure and subsequent review of the Devices as well as the forensic examination of the Devices consistent with the warrant. The examination will require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

11. Following the issuance of this warrant, an agent will seize the Devices and submit the Devices for a forensic extraction of the Devices. Subsequently, the forensic extraction will be examined for evidence described in Attachment B. All searches and forensic analysis of the data contained within the Devices and its memory cards will employ search protocols directed exclusively to the identification and extraction of data within the scope of this warrant. If evidence relating to another crime is discovered, agents will not look for additional evidence relating to the new crime without first applying for and obtaining a search warrant for that new crime.

12. Based on the foregoing, identifying and extracting data subject to seizure pursuant to this warrant may require a range of data analysis techniques, including manual review, and, consequently, may take weeks or months. The personnel conducting the identification and extraction of data will complete the analysis within one-hundred twenty (120) days, absent further application to this court.

## TRAINING AND EXPERIENCE ON DIGITAL DEVICES

13. As used herein, the term "digital device" includes any electronic system or device capable of storing and/or processing data in digital form, including: Central Processing Units (CPU's or "computers"); laptop or notebook computers; personal digital assistants; USB hard drives

or "jump drives" intended for removable media; digital camera or removable media storage cards; external hard disk drives, cellular telephones, GPS devices, compact disks (CD, DVD, and Blu-Ray); internal flash medium; and security devices.

14. In searching digital data stored on digital devices, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel will complete the search as soon as is practicable but not to exceed 120 days from the date of execution of this warrant. If additional time is needed, the government may seek an extension of this time period from the Court within the original 120-day period from the date of execution of the warrant.

b. The team searching the digital devices will do so only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The team may subject all of the data contained in the digital device or the forensic copy capable of containing items to be seized as specified in this warrant to the protocols to determine whether the digital device and any data falls within the items to be seized as set forth herein. The team searching the digital device may also search for and attempt to recover "deleted," "hidden" or encrypted data to determine, pursuant to the protocols, whether the data falls within the list of items to be seized as set forth herein.

ii. These search protocols also may include the use of tools to exclude normal operating system files and standard third-party software that do not need to be searched.

c. When searching a digital device pursuant to the specific search protocols selected, the team searching the digital device shall make and retain notes regarding how the search was conducted pursuant to the selected protocols.

d. If the team searching a digital device pursuant to the selected protocols encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that digital device pending further order of Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

e. At the conclusion of the search of the digital devices, any digital device determined to be itself an instrumentality of the offense(s) and all the data thereon shall be retained by the government until further order of court or one year after the conclusion of the criminal case/investigation.

f. Notwithstanding, after the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized in this warrant on any retained digital devices or digital data absent further order of court.

g. If the search team determines that a digital device is not an instrumentality of any offense under investigation and does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will as soon as practicable return the digital device and delete or destroy all the forensic copies thereof.

h. If the search determines that the digital device or the forensic copy is not an instrumentality of the offense but does contain data falling within the list of the items to be seized pursuant to this warrant, the government either (i) within the time period authorized by the Court for completing the search, return to the Court for an order authorizing retention of the digital device and forensic copy; or (ii) retain only a copy of the data found to fall within the list of the items to be seized pursuant to this warrant and return the digital device and delete or destroy all the forensic copies thereof.

## IDENTIFICATION OF THE ITEM TO BE SEARCHED

15. The property to be searched are a Black Samsung phone in clear case, IMEI: 358284143661740 (Device 1); Black Samsung phone, IMEI: 353021070606008 (Device 2); Silver HP computer, model Elite X2, Serial number: CND122ONHS (Device 3), that are currently in the Yellowstone County Sheriff's Office evidence vault. referred to as the "Devices," as described in Attachment A.

16. This warrant application seeks permission to seize and search the aforementioned Devices for the evidence, contraband, fruits, or instrumentalities of crimes described in Attachment B. The applied-for warrant would also authorize any forensic examination of the Devices which may take place outside of or inside of the State of Montana.

## PROBABLE CAUSE

17. In January 2024, Detective Bethany Richter of the Yellowstone County Sheriff's Office, while acting in an undercover capacity, posted a Whisper message saying "Booooored". A suspect with the username of "Eagle_Tiger" responded to the post and engaged in conversation with Det. Richer's undercover persona. Det. Richer identified her persona as a 12-year-old female and "Eagle_Tiger" identified himself as a 42-year-old male named Andrew from Alberta, Canada. Once Andrew discovered the persona's age, he immediately started talking about being a "pervert" and wishing to be the persona's "inappropriate daddy." Andrew eventually asked Det. Richter for a phone number and on January 27, 2024, Andrew began a text conversation with Det. Richter's undercover persona.

18. During the course of the text conversation, Andrew bragged about sleeping with a 16-year-old female and about getting some ladies in their 20s pregnant. Andrew texted that these ladies eventually had abortions. Andrew mentions several times in the text conversation that he is 42 and is texting an "almost teenager", clearly indicating he knows the age of the undercover persona. Andrew includes a photograph in this portion of the text conversation, which shows a male from the chest down to his boxers who appears to have an erection. Andrew then gets the date of birth of the undercover persona (2011) and asks if Det. Richter's undercover persona can "imagine 1981 dick in 2011 pussy".

19. Andrew and Det. Richter's undercover persona also engage in conversations on the app Kik, where Andrew uses the username "A B". On Kik, Andrew constantly talks about impregnating Det. Richter's undercover persona and says he is planning his upcoming visit to Billings, Montana around the undercover persona's period for the best opportunity to impregnate her.

Andrew stated several times he will likely go to jail if he impregnates the persona. Andrew and the persona often talk about the age difference. For example, Andrew states he is "going to end up with 12 yr old pussy on my married daddy dick." Andrew has sent pictures of his penis, has asked for nude pictures in return; he has discussed sexual activities things he wants to do to the undercover persona such as spanking her then having sex with her. Andrew has also sent approximately eight videos that appear to contain Child Sexual Abuse Material (CSAM) and said this will be his "summer of being a pervert daddy". The CSAM videos depict children that Detective Richter estimate being 6-14 years of age, being raped by adult males. The persona asked Andrew where he found the CSAM he was sending to her and he said, "Get a pervert to show you."

20. Andrew also stated he was arranging a date with a 15-year-old female he met on Reddit however Andrew later stated he got "stood up" which caused him to create his plans to come to Billings, Montana to meet with the undercover persona. As of the weekend of May 4-5, 2024, Andrew Scott BROWN stated he wished the persona to wear only knee-high socks at the hotel he reserved for the visit. Andrew Scott Brown stated after that he believes, "the conclusion will be big thick daddy dick getting a first taste of young pussy." He later stated, "I want to try to fit in in. We'll go slow, I promise." During the course of conversation, Andrew talked about bringing the undercover persona a new phone so the two could communicate more and she could send photos as she stated her screen was cracked on her current phone, preventing her from taking pictures. Andrew also mentioned his wife found evidence of his unfaithfulness via old emails.

21. Based on information obtained from other law enforcement agencies, I believe "Eagle_Tiger" and Andrew to be Andrew Scott BROWN with a date of birth of 04/26/1981. Andrew is a resident of Sylvan Lake, Alberta, Canada. Andrew advised Det. Richter's undercover persona

that he was traveling to Billings, Montana on May 6, 2024, with intentions of staying until May 8, 2024. Det. Richter has confirmed that Andrew made a reservation at the C'mon Inn in Billings, Montana for May 6-8, 2024. On May 6th, 2024, Andrew traveled to Billings, MT and was arrested by local law enforcement. A test Kik message was sent to his phone, which showed a notification from Kik.

22. Once Andrew was arrested, his black Samsung phone in clear case, IMEI: 358284143661740 (Device 1) was taken off his person. Detective Richter applied for and was granted a Montana District Court warrant for Andrew's vehicle. Upon searching Andrew's vehicle a black Samsung phone, IMEI: 353021070606008 (Device 2) and a silver HP computer, model Elite X2, Serial number: CND122ONHS (Device 3) were discovered and seized. These items are currently in the Yellowstone County Sheriff's Office evidence vault. All of the evidence was originally seized by the Yellowstone County Sheriff's Office (YCSO) and will remain in YCSO custody until such time that a search warrant could be applied for and granted.

23. The affiant's training and investigative experience in the area of Sexual Abuse of Children and Child Sexual Abuse Material has led the affiant to conclude that probable cause exists to suggest that evidence of violations of the "Relevant Statutes" will be present on the three Devices. Most sexual abuse suspects utilize their smartphones to capture images/videos from the internet for sexual gratification purposes, to disseminate these CSAM images and videos to others, and to arrange meeting times and places for the purposes of sex with children. Laptop computers are also often utilized to view and download CSAM from the internet and facilitate communication with children for the purposes of sex. Sometimes, computers are used to frequent websites for commercial sex advertisements, laptop computers can be a more convenient method for posting and accessing the

internet for posting of advertisements and/or communicating with customers or pimps. Thus, the affiant believes that probable cause exists to suggest that evidence of violations of the relevant statutes will be present on the three Devices.

## CONCLUSION

Since the Devices are also an instrumentality of the relevant crimes, the affiant submits that the facts outlined in this affidavit support probable cause for the issuance of a search and seizure warrant authorizing the examination of the Devices to seek the items described in Attachment B. Assistant United States Attorney Zeno Baucus concurs with this assessment.

Respectfully submitted,

Bethany A. Richter
FBI TFO/Yellowstone County Detective

Sworn and subscribed before me this 17 day of May, 2024.

Timothy J. Cavan
United States Magistrate Judge